

Побег из Шоушенка в мире сетей

Александр Попов
VK Cloud





Кто мы – VK Cloud

Инфраструктура (IaaS)

Виртуальные серверы

Гибкие конфигурации, неограниченное количество IP и безлимитный трафик в 1 ГБит/с.

Дисковые хранилища

Блочные (HDD, SSD) и объектные (S3). Классические хранилища или SDS (CEPH)

Виртуальные сети

Единая локальная сеть для серверов, приватный и публичный DNS, балансировка нагрузки и VPN.

Back-up и DR

Автоматическое восстановление IT-инфраструктуры в случае аварии

Платформа (PaaS)

Кластеры Kubernetes

Автоматическое масштабирование приложений и выстраивание быстрых DevOps-процессов.

Managed-базы данных

Полная автоматизация жизненного цикла работы СУБД: MySQL, PostgreSQL, MongoDB, Redis, Postgres Pro, ClickHouse, Arenadata DB, Tarantool Cloud

Cloud Big Data

Преднастроенные инструменты для хранения, обработки и анализа больших данных

Cloud ML Platform

Платформа для полного цикла ML-разработки и совместной работы Data-команд

Маркетплейс

Сервисы партнеров VK

Расширяющаяся экосистема решений на единой платформе

Сервисы VK

Прикладное ПО и программы для разработчиков





Облака – объективная реальность

- Пандемия
- Санкции
- Экономический кризис
- Бизнесу ~~выгодны~~ необходимы облака
- Разработчики должны решать задачи бизнеса
- Разработчики разбираются с облаками





“Запчасти” облаков

- SaaS
- PaaS
- IaaS
  - Виртуальные сервера
  - Виртуальные диски
  - **Виртуальные сети**





SDN. Зачем это?

- Доступ до соседних виртуальных серверов
- Доступ в интернет
- Изоляция от соседей





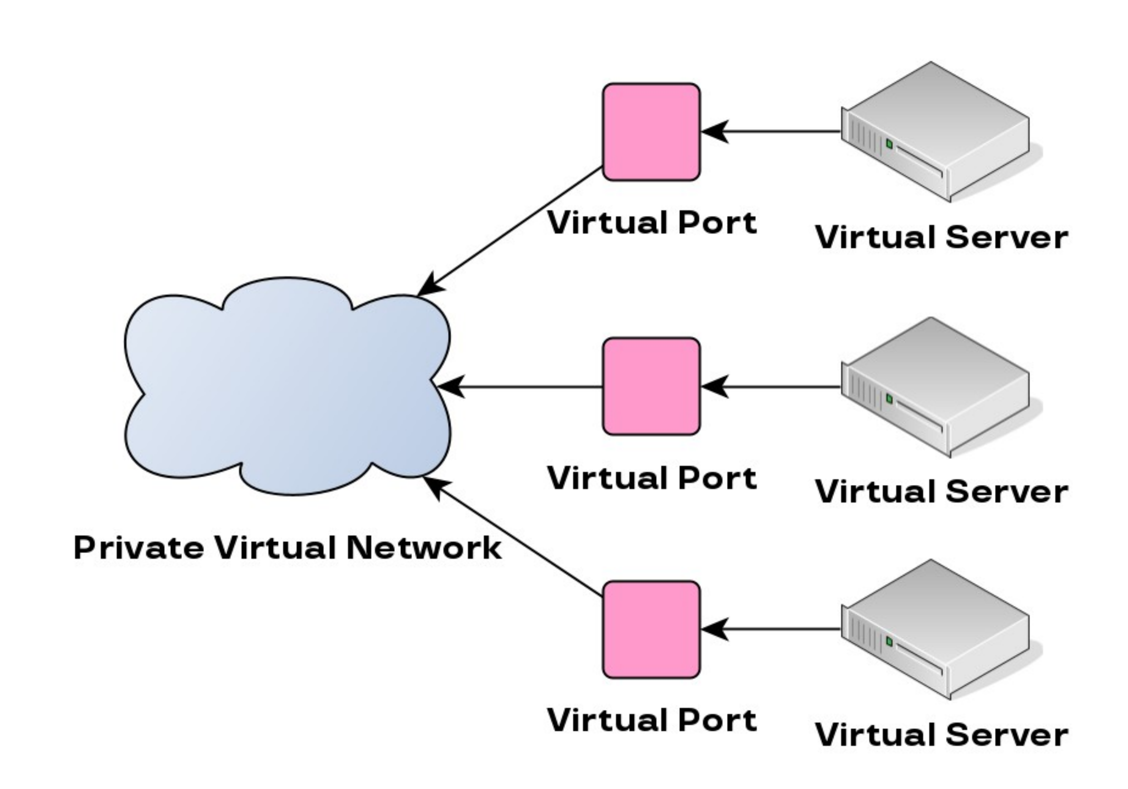
Какой SDN мы используем



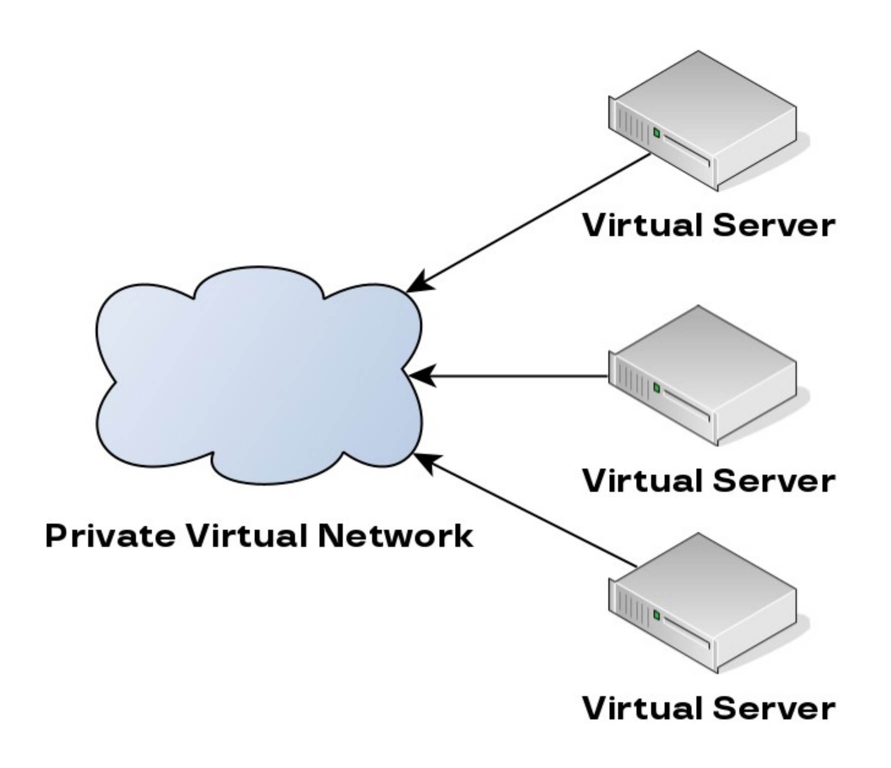




Основные сущности Neutron



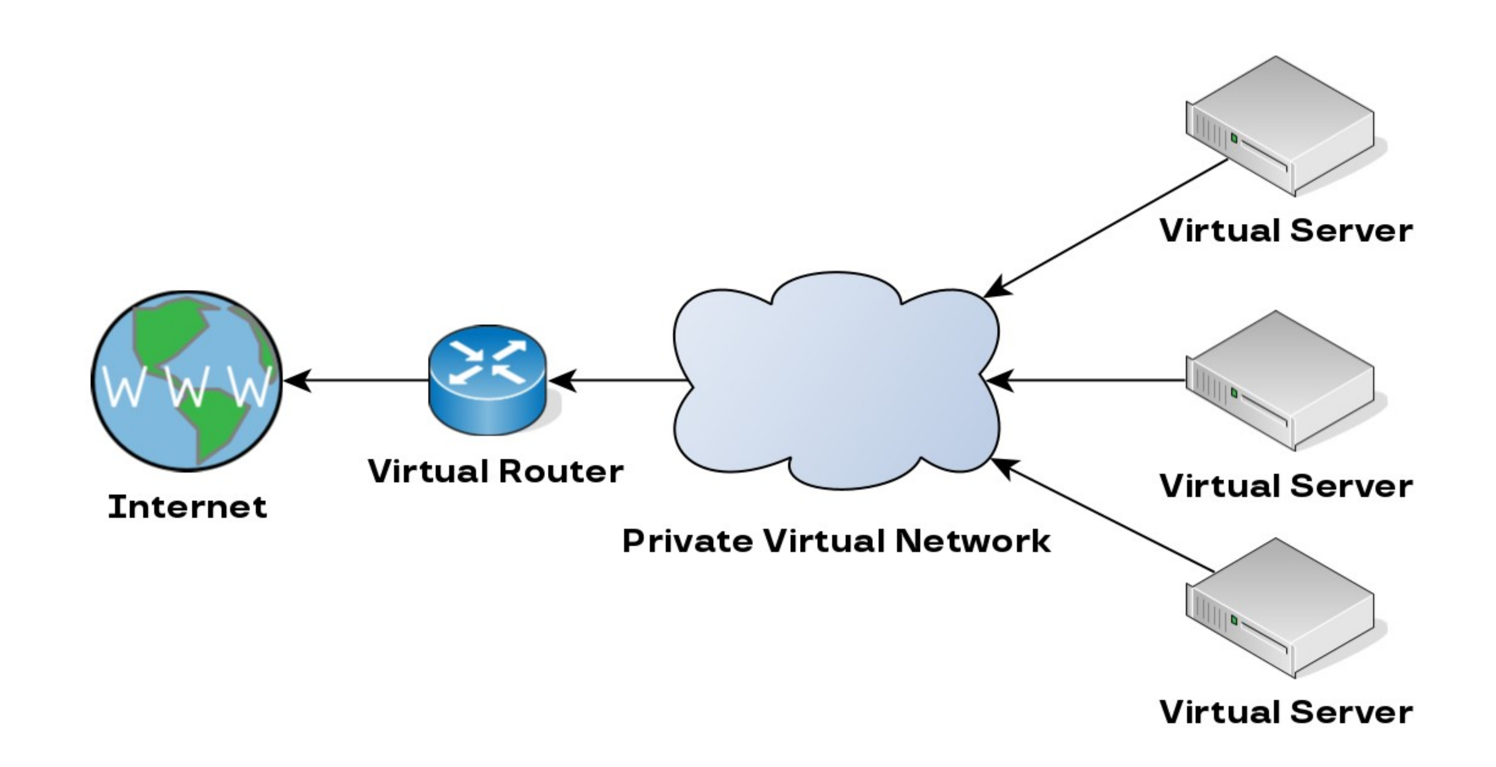
Простейшая связность VM







Типичная конфигурация сети клиента

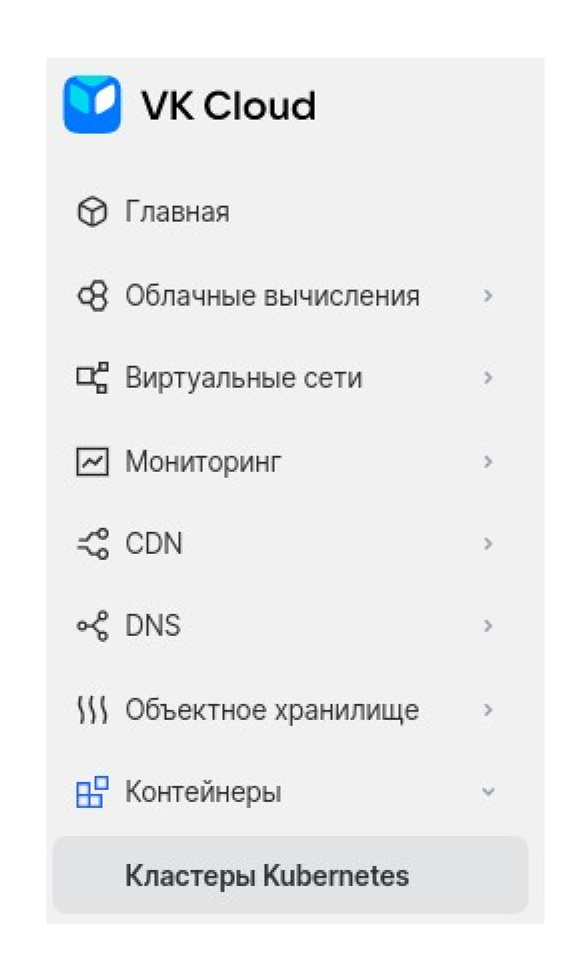






Модно-молодежно

- Современные задачи требуют современных решений
- Всем нужно CI/CD
- VK Cloud предоставляет большой набор PaaS-сервисов
- Среди них есть и K8S as a Service







Использование K8S в облаках

Virtual Server
Virtual Server
Virtual Server
Internet
Virtual Router
Private Virtual Network
K8S

Работа PaaS-сервисов

VK Cloud
API

Virtual Server

Internet

Virtual Router

Private Virtual Network

Virtual Server

K8S

Virtual Server

Работа PaaS-сервисов

Virtual Server

VK Cloud API

Virtual Server

Internet

Virtual Router

Private Virtual Network

Virtual Server

K8S

Virtual Server

Соединение с инфраструктурой клиента

Real Server

Internet

Virtual Server

Client DC

Gateway Router

Virtual Router

Private Virtual Network

Virtual Server

K8S

Virtual Server





Соединение с инфраструктурой клиента

Real Server
Internet
Virtual Server
VPN
VPN
Virtual Server
Gateway Router
Virtual Router
K8S
Client DC
Private Virtual Network
Virtual Server





ИБ в облаках


Подключение к облаку через VPN
Выделенный канал к облаку
imgflip.com


VK Cloud


HL
HighLoad++
2022

Соединение с инфраструктурой клиента

Real Server

Client DC

Gateway Router

Internet

Dedicated Channel

Virtual Router

Private Virtual Network

Virtual Server

Virtual Server

Virtual Server

K8S





Соединение с инфраструктурой клиента

Real Server
Internet
Virtual Router
VK Cloud API
Virtual Server
Dedicated Channel
Gateway Router
Client DC
Private Virtual Network
Virtual Server
K8S
Virtual Server

ИБ: аппетит приходит во время еды

- Обеспечивать безопасность двух роутеров сложнее, чем одного





ИБ: аппетит приходит во время еды

- Обеспечивать безопасность 2х роутеров сложнее, чем одного
- Virtual router – несертифицированный firewall





ИБ: аппетит приходит во время еды

- Обеспечивать безопасность 2х роутеров сложнее, чем одного
- Virtual router – несертифицированный firewall
- Клиент расширяет свою сеть в облако, но с теми же требованиями к безопасности





Изолированная от Internet сеть

Real Server

Internet

VK Cloud API

Virtual Server

Dedicated Channel

Gateway Router

Client DC

Private Virtual Network

Virtual Server

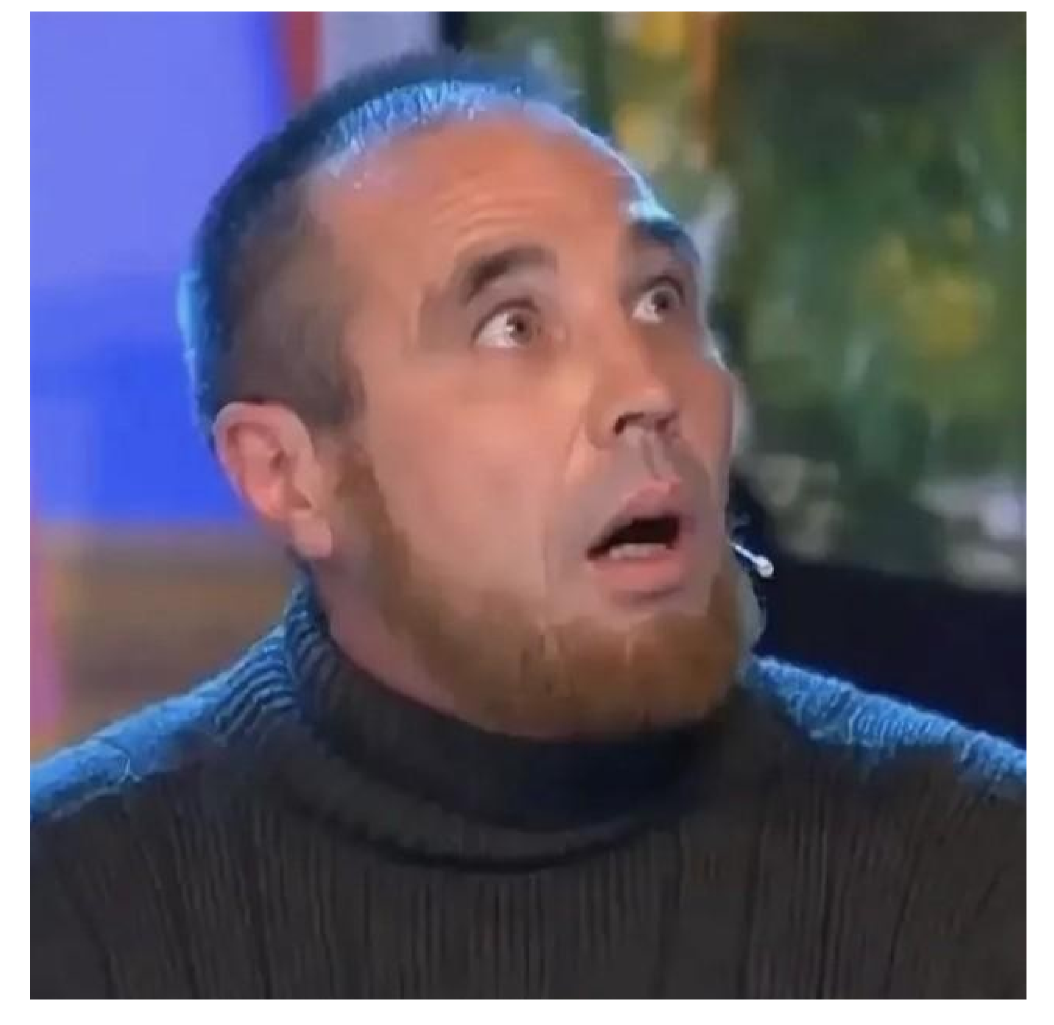
K8S

Virtual Server





Команды разработки VK Cloud



Настоящее расположение IaaS API

VK Cloud API

VK Cloud Internal Network

Real Server

Internet

Client DC

Gateway Router

Dedicated Channel

Private Virtual Network

Virtual Server

Virtual Server

Virtual Server

K8S





Задача: Выйти из overlay сети вовне





Целевая схема!





А как сбежать?

- Самый простой способ сбежать из тюрьмы – не попадать в нее





А как сбежать?

- Самый простой способ сбежать из тюрьмы – не попадать в нее
- В случае overlay сети взаимодействие с внешним миром происходит в точках подключения





А как сбежать?

- Самый простой способ сбежать из тюрьмы – не попадать в нее
- В случае overlay сети взаимодействие с внешним миром происходит в точках подключения
- Точки подключения к Virtual Network – Virtual Port





Точки подключения к overlay

DHCP
Virtual Port
Virtual Port
Virtual Server
Virtual Router
Virtual Port
Virtual Port
Virtual Server
Private Virtual Network
Virtual Port
Virtual Server





Вспоминаем схему внутренней сети

VK Cloud API

VK Cloud Internal Network

Real Server

Internet

Client DC

Gateway Router

Dedicated Channel

Private Virtual Network

Virtual Server

Virtual Server

Virtual Server

K8S





Вариант решения проблемы

Real Server
Client DC
Gateway Router
Internet
WWW
Dedicated Channel
VK Cloud API
VK Cloud Internal Network
Private Virtual Network
Virtual Port
Virtual Server
Virtual Port
Virtual Server
Virtual Port
Virtual Server
K8S

Shadowport





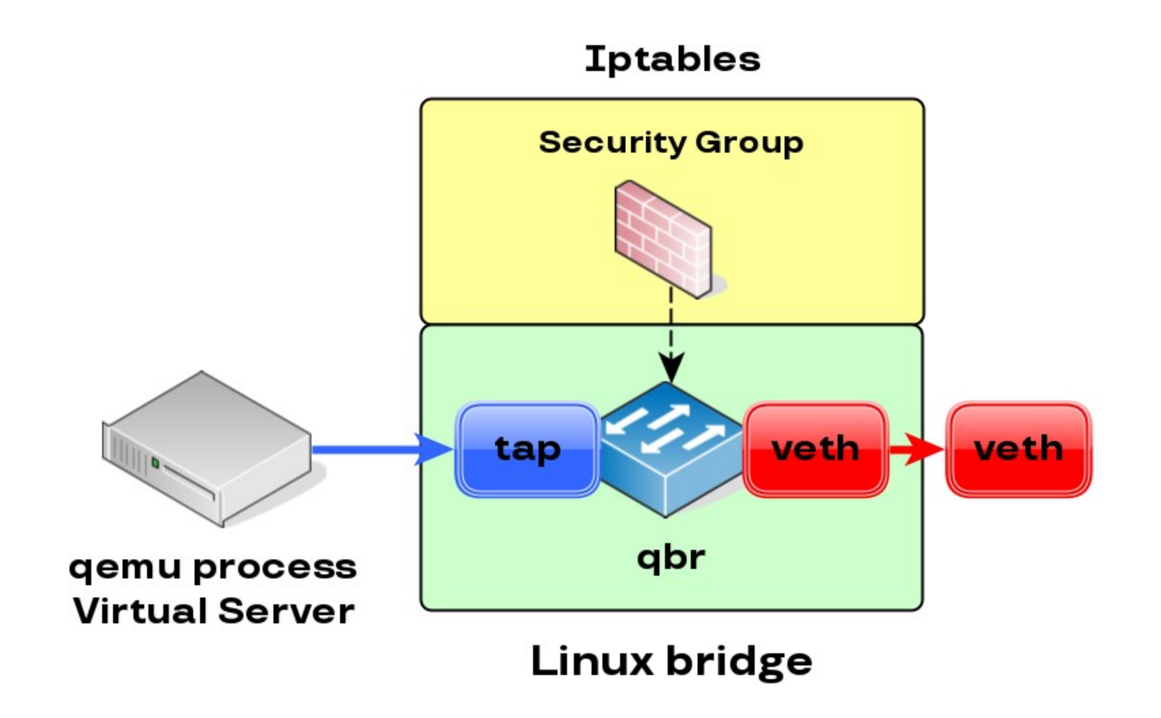
Устройство Virtual Port на Dataplane







Устройство Virtual Port на Dataplane







Устройство Virtual Port на Dataplane

Iptables

Security Group

VXLAN

br-tun

tap

veth

veth

qbr

br-int

qemu process
Virtual Server

Linux bridge

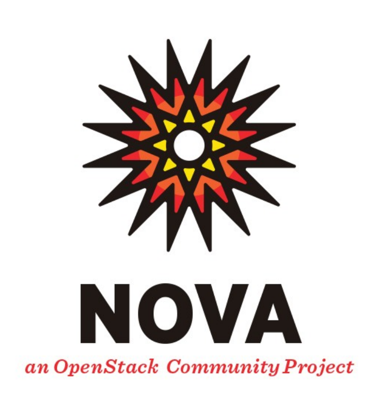
Open vSwitch





Разделение ответственности

- За создание виртуальных машин и управление ими отвечает Nova







Разделение ответственности

- За создание виртуальных машин и управление ими отвечает Nova



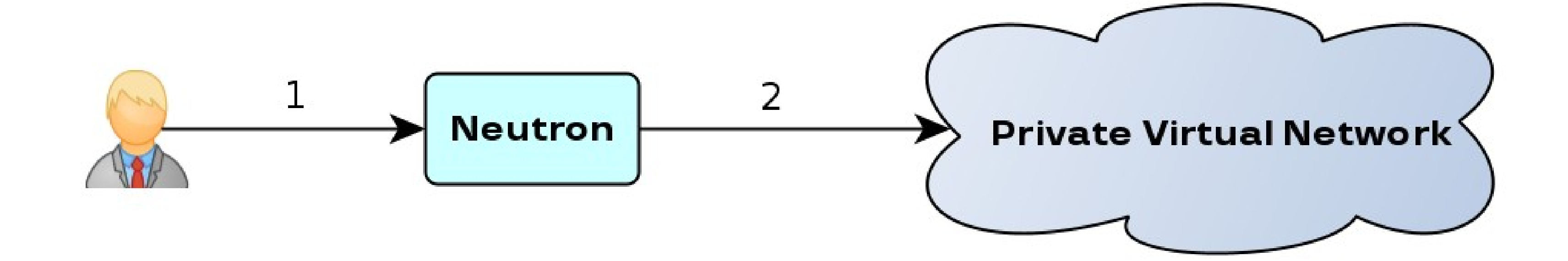
- За создание сетевых сущностей и управление ими отвечает Neutron







Взаимодействие на Control Plane







Взаимодействие на Control Plane

1 Neutron 2 Private Virtual Network

3 Nova 4 Virtual Server





Взаимодействие на Control Plane

1
Neutron
2
Private Virtual Network
6
5
Virtual Port
3
Nova
4
Virtual Server





Ответственность на Dataplane

Iptables

Security Group

qemu process
Virtual Server

tap

qbr

veth

veth

br-int

br-tun

VXLAN

Linux bridge

Open vSwitch

Nova

Neutron

Дополнительная фильтрация на Dataplane

Iptables

Security Group

qemu process
Virtual Server

tap

qbr

veth

Linux bridge

NAT

Filter by dst_ip

veth

shadowport

br-int

br-tun

Open vSwitch

VK Cloud
API

VXLAN

Nova

Neutron

Чья это будет зона ответственности?

- Сделать это зоной ответственности Nova





Чья это будет зона ответственности?

- Сделать это зоной ответственности Nova
  - Nova ничего не знает о сетях





Чья это будет зона ответственности?

- Сделать это зоной ответственности Nova
  - Nova ничего не знает о сетях
- Сделать это зоной ответственности Neutron





Чья это будет зона ответственности?

- Сделать это зоной ответственности Nova
  - Nova ничего не знает о сетях
- Сделать это зоной ответственности Neutron
  - Править код Neutron долго и сложно





А действительно ли у нас такой выбор?





Чья это будет зона ответственности?

- Сделать это зоной ответственности Nova
  - Nova ничего не знает о сетях
- Сделать это зоной ответственности Neutron
  - Править код Neutron сложно
- Сделать это зоной ответственности третьего сервиса



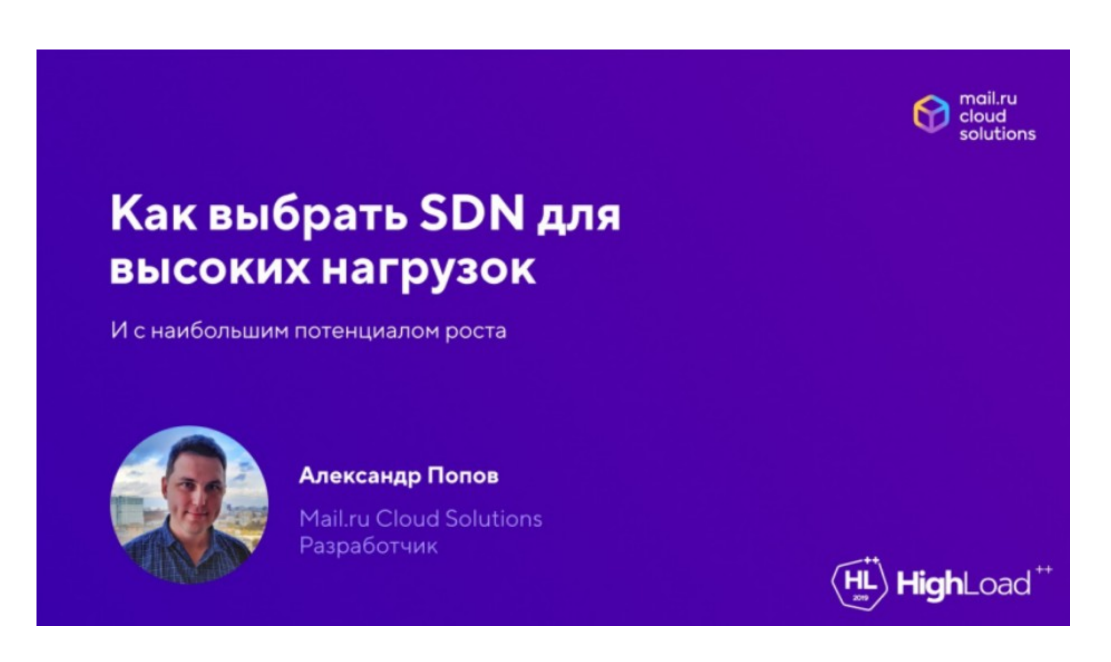


По счастливой случайности…

У нас есть еще один SDN – **Sprut**

Мы готовимся заменить Neutron на него

bit.ly/3EMDdCx







Ответственность на Dataplane

Iptables

Security Group

NAT

Filter by dst_ip

VK Cloud API

VXLAN

tap

veth

veth

br-tun

qemu process Virtual Server

qbr

shadowport

br-int

Linux bridge

Open vSwitch

Nova

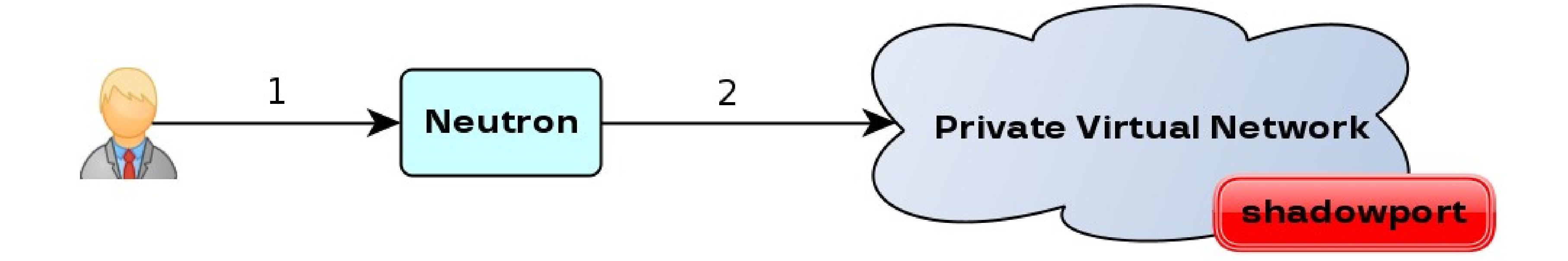
Sprut

Neutron





Новое взаимодействие на Control Plane







Новое взаимодействие на Control Plane

1
Neutron
2
Private Virtual Network
shadowport
3
Nova
4
Virtual Server





Новое взаимодействие на Control Plane

1
Neutron
2
Private Virtual Network
shadowport
6
7
Virtual Port
vif=shadowport
5
Sprut
Shadowport
3
Nova
4
Virtual Server



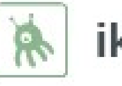


Не единственный путь

Коллеги из Huawei сделали

Node-Local Virtual IP

bit.ly/3Ou7Dwv



ikeeip 28 февраля в 18:02

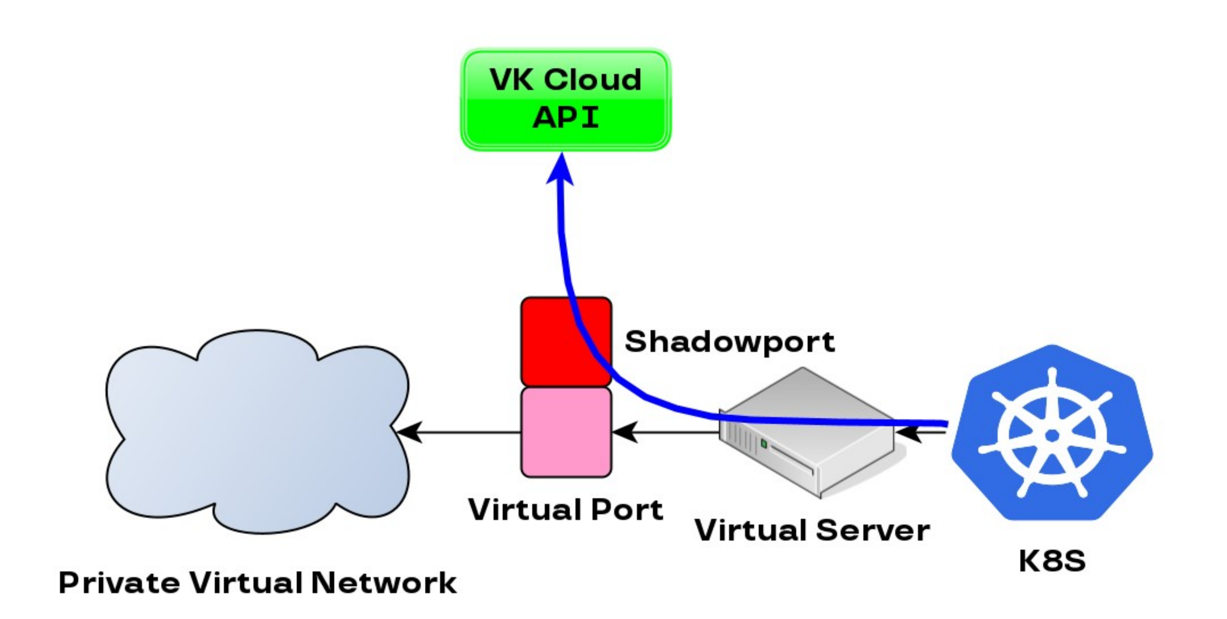
Node-Local Virtual IP в OpenStack

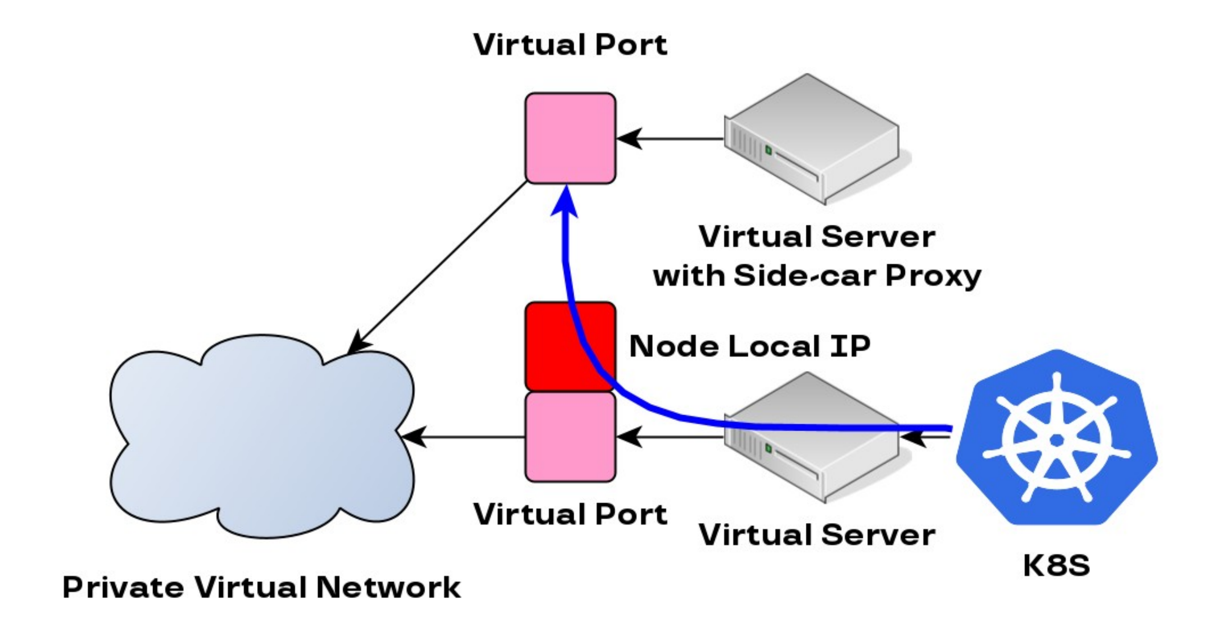
Блог компании Huawei, Open source*





Сравнение с Node-Local Virtual IP









Взаимодействие с OpenSource не быстрое



Overview Code **Bugs** Blueprints Translations Answers

[RFE] Add support for Node-Local virtual IP

Bug #1930200 reported by Ilya Chukhnakov on 2021-05-31

OpenStack Infra (hudson-openstack) wrote on 2022-04-01: **Related fix merged to neutron-lib (master)**	#44





Выводы

- Полезно понимать работу облаков в современном мире
- Можно изменять в нужную сторону работу OpenStack, если понимаешь его устройство
- При этом не обязательно глубоко модифицировать сам OpenStack





Спасибо за внимание!

Доклад про Sprut
bit.ly/3EMDdCx

Статья про Node Local IP
bit.ly/3Ou7Dwv



Оставляйте обратную связь по докладу



